Palm Bay police Department CR# 19-008449

05-2019-CF-042107-AXXX-XX

IN THE CIRCUIT COURT
OF THE EIGHTEENTH JUDICIAL CIRCUIT
IN AND FOR BREVARD COUNTY, FLORIDA

FILED IN PALM BAY
CLERK OF CIR. CT.
BREVARD CO., FL.
2019 SEP 23 P 4:24
SCOTT ELLIS

AFFIDAVIT FOR SEARCH WARRANT – DIGITAL EVIDENCE

State of Florida
County of Brevard

BEFORE ME, MARLENA HENTSCHEL a sworn law enforcement officer, personally came **Detective Jennifer Graves #125** of the Palm Bay Police Department, who being first duly sworn, deposes and says: That the Affiant is a citizen of Brevard County, State of Florida, and that she has reason to believe and does believe that the following digital device contains evidence of a felony crime(s), to wit: F.S. 800.04(5)(a) Lewd or Lascivious Molestation, F.S. 800.04(7) Lewd or Lascivious Exhibition and F.S. 847.0135(3)(a) Certain Uses of a Computer Prohibited.

The digital device is described as follows: blue and black Samsung Galaxy Note 9 smartphone, entered into Palm Bay Police Department property and evidence under item #JA5. This digital device was seized when it was consensually given to police by [redacted] The digital device is located as follows: Palm Bay Police Department, 130 Malabar Rd. SE, Brevard County, Florida. To reach the premises where the digital device is located one would begin at the intersection of Malabar Rd. and Minton Rd. in the city of Palm Bay, proceed east on Malabar Rd. for approximately 300 feet. Palm Bay Police Department is located directly to the south, 130 Malabar Rd. SE Palm Bay, Florida.

This affidavit for the search warrant sets forth the facts, which establish probable cause for the affiant to believe that there is now on, in, at, or within the above-described digital device (including SIM card(s), memory card(s), and flash memory card(s)) items related to the above-mentioned offense(s) that occurred in Brevard County, Florida, to wit:

1. Electronic address books and information
2. Incoming and outgoing call detail logs
3. Digital photographs
4. Video
5. Text messages (SMS, MMS) in the user's inbox, sent, saved, and trash folders
6. Contents of communications, including file attachments, in the user's email inbox, sent email, saved email, and email trash folders
7. Contents of communications, including file attachments, associated with the user's third-party messaging or social media applications.
8. Files showing ownership, possession, or control of digital device and associated storage disks
9. System data information and device identification information (i.e. serial number, IMEI number) related to the digital device
10. Files associated with the device listed above, including password protected files, both text and image types that may include, but are not limited to: ".doc, .txt, .gif, .bmp,

.tif, .pcs, .pic, .png, .dcs, .art or .jpeg.", that can be stored or saved by these suffixes or they can be renamed and saved under different titles

11. System application data or network data, including logs

The facts tending to establish grounds for this application and the probable cause of believing that such facts exist are as follows:

On 08/17/2019, [redacted] year old EM was brought in by her mother to report Lewd or Lascivious crimes by [redacted] Joshua Mills, against her. EM stated that the following crimes took place [redacted] She stated essentially the following: that for the past 8 to 12 months Mr. Mills has been masturbating in front of her, allowing her to see pornography, has touched her bare breast and has sent her masturbating videos of himself along with penis pictures. EM stated that he messages her these things along with various typed messages by means of the gaming application DISCORD. She said he has asked her to "help him" with his masturbation, has sent her a photo of a box of condoms and then implied that if they had sex it would be safe. EM says that Mr. Mills has emotional problems as well and constantly threatens to kill himself or talks about leaving and never coming back, that no one likes him, and he should die. EM said that this is how he kept her from telling her mother what was going on, by manipulation that he would kill himself. EM said that Mr. Mills also has rage outbursts and he throws things and yells. EM said she was in fear he may hurt [redacted] or himself. Today, 08/17/2019, Mr. Mills again contacted her through DISCORD and said, "I could kiss you all over and make your heart beat really fast", "I want to give you love and affections". EM replied to him that she wanted him to stop, that she is just a kid and that when he talks to her that way it makes her very uncomfortable. Mr. Mills responded to her by saying he wanted to die, that he's a piece of "shit" and is needy. Mr. Mills called himself ugly, useless to everyone and worthless. Again, EM asked him to stop and reminded him that she is a child. EM said that her DISCORD "username" is dumb bitch juice#2692 and Mr. Mills's username is Enemy Crab#9763. She stated that Mr. Mills utilizes his cell phones and laptop computer to message through DISCORD.

On this same date, 08/17/2019, Mr. Mills was Baker Acted and brought to the police station. Post-Miranda, Mr. Mills stated that he has messaged EM on DISCORD and did write those messages from today. Mr. Mills didn't have an excuse for his messaging EM other than stating it was a response to something she said yesterday but understood it was inappropriate to send to EM. Mr. Mills did say he said he wanted to kill himself and he does say that all the time. Mr. Mills stated that his "username" on DISCORD is Enemy Crab#9763 and EM's is dumb bitch juice#2692. Mr. Mills denied all other Lewd or Lascivious crimes.

Mr. Mil[redacted] stated that she knows both EM and Mr. Mills use DISCORD to message. She stated that Mr. Mills and EM both got new phones and new phone numbers in the last week or so. She stated that Mr. Mills utilized his new phone, Samsung Galaxy S10 and his old phone, Samsung Galaxy Note 9 to utilize DISCORD. She said he also used his HP laptop.

[redacted] gave police all of EM's media; Samsung Galaxy S8, Samsung Galaxy S10 and a HP computer tower. She also gave police Mr. Mills old Samsung Galaxy Note 9 and HP laptop. Mr. Mills current cell phone, Samsung Galaxy S10, was taken from Mr. Mills during his arrest.

[redacted] and EM wish to pursue charges.

Your affiant certifies that she is conducting an ongoing criminal investigation into the following offense(s) of F.S. 800.04(5)(a) Lewd or Lascivious Molestation, F.S. 800.04(7) Lewd or Lascivious Exhibition and F.S. 847.0135(3)(a) Certain Uses of a Computer Prohibited. Your affiant states that there is Probable Cause based on the above-stated facts that the target digital device is now being kept or used in violation of the laws of State of Florida or constitutes or contains evidence relevant to proving that a felony has been committed, to wit: F.S. 800.04(5)(a) Lewd or Lascivious Molestation, F.S. 800.04(7) Lewd or Lascivious Exhibition and F.S. 847.0135(3)(a) Certain Uses of a Computer Prohibited.

Your Affiant, **Detective Jennifer Graves #125**, is certified by the State of Florida Commission of Criminal Justice Standards and Training as a Law Enforcement Officer as the result of her attendance and completion of the Brevard County Law Enforcement Academy in 1997 and is now employed in and for the City of Palm Bay Police Department, sworn on April 26, 1999. Your Affiant is an experienced Police Officer with over 20 years with the City of Palm Bay, with 10 of those years as a Traffic Homicide Investigator. Your Affiant has investigated and made arrests on numerous felony investigations involving Aggravated stalking, child pornography, sexual battery, attempted murder, homicide, narcotics, and other felony offenses. Your Affiant has attended numerous schools and studied various course materials during the past years to include but not limited to, Sex Offense Investigations, Death Investigations, and crimes against persons, crimes against property, interview and interrogations, crime scene analysis and attended the Detective Academy. Your Affiant has written, assisted with, or executed multiple arrest and search warrants. Your Affiant was assigned to the Uniform Service Division-July 1999, the CNT team in 2002, and Special Victims Unit in 2015 as a Detective.

Sent and received electronic text messages, both incoming and outgoing phone numbers, stored on the suspect's digital device can be retrieved at a later date. Text messages which are sent from the users digital device to another digital device are stored in the "outbox", text messages received are stored in the "inbox". Messages both sent and received are stored in the digital device's memory and will remain there even if the power and/or service is shut off to the digital device. This same application also applies to photographs and videos, which are sent and received between digital device. The incoming photographs and videos, depending on the type of digital device, are also stored in the "inbox" while outgoing photographs and videos are stored in what is referred to as a media gallery. As with text messages, the images are stored on the device until manually deleted. Incoming and outgoing phone numbers are saved on a call log. These numbers remain until manually deleted. Even deleted data or information on a device can possibly be recovered by forensic measures.

System data is information that is stored by and changed by the digital device itself based on inputs by the user; however, the user cannot directly manipulate or otherwise change the information. In order for a successful forensic examination of a digital device, system data information is almost always required to be extracted from the digital device. Such information is used to identify the digital device and interpret data extracted from said device.

During the forensic examination process, it is often required for the examiner to extract all digital data – not just the target data – from the digital device. Users may store information or images in random order with deceptive file names, which requires searching authorities to examine all the stored data to determine whether it is included in the warrant. However, the forensic examiner and/or Affiant will limit his or her review of the extracted to just what is authorized herein and by the Court in its approved search warrant(s).

Your Affiant is seeking evidence of ownership, use, and identification, and knows that ownership and control of a computer and/or a digital device can be placed at issue through a simple denial, "that is not mine." In your Affiant's training and experience, some of the best ways to establish control are by searching the calendar, contacts, photo/video galleries, communications, settings, and social networking activity. The calendar often contains appointments specific to an individual such as birthdays and doctor appointments. Contacts often contain friends and associates specific to an individual such as mom, dad, dentist, etc... Photo/video galleries often contain selfie photos/videos that clearly depict the owner/holder of the phone. Communications via messages and emails often identify the sender/recipient of the communication by name. Additionally, the context of the communications often identifies the sender and/or recipient. Settings often contain user names, addresses, and phone numbers, Wi-Fi network tables, associated wireless devices(such as known Wi-F networks and Bluetooth devices), associated connected devices (such as for backup and syncing purposes), stored passwords, and user dictionaries that can identify the owner/user of the device. Therefore, your Affiant is seeking all of the above information to establish ownership and control of the device.

The process of analyzing digital device takes on many forms. Many times the analysis of a mobile device can be completed by connecting the device to forensic applications, which will gather the data contained within that device. Although this is the first and primary means of analyzing digital device, there are instances where utilizing this non-destructive means is impossible. If a digital device is protected by a password (that is not supplied by the suspect or a password that cannot be bypassed by forensic applications) it may still be possible to retrieve data. It may also be possible to extract data from digital devices that are designed to not connect with computers or forensic applications. There are additional processes which have been described to me by forensic experts, including:

1. Connecting the device to forensic applications, which will gather the data contained within that device.
2. Removing the circuit board from the digital device and soldering wires to points used by the manufacturer ["JTAG"]. These points allow direct access to the memory on the digital device. This process may cause damage to the digital device, but typically the digital device will remain intact and functional when put back together.
3. Removing the flash memory chip on the digital device that actually stores the data on the digital device. Once the chip is removed, forensic experts can read the data directly from the chip ["Chip-Off"]. This process will likely result in the permanent destruction of the digital device; however, it allows for access to the data that was located on the digital device. It is my training and experience that each of the methods described above for extraction will result in an accurate representation of some or all of the available data from the digital device itself.

WHEREAS, your affiant requests authorization to utilize the various recognized processes to analyze the above-described device including 1) connecting the device to forensic applications, which will gather the data contained within that device, 2) removing the circuit board from the digital device and soldering wires to points used by the manufacturer and directly accessing the memory on the digital device ["JTAG"] which may result in damage to the digital device, and 3) removing the flash memory chip on the digital device that actually stores the data on the device and reading the data directly from the chip ["Chip-Off"] which will likely result in the permanent physical destruction of the device while still allowing access to the data that was stored on the device. Your affiant request authorization to utilize the least destructive means to analyze the device before using more potentially destructive methods described in this paragraph, if necessary.

And further, your Affiant makes this Affidavit and prays for the issuance of a search warrant in due form of law for the search and examination of the digital device described above with such lawful assistance as may be necessary, to include forensic computer analyst experts or any other assistance that may be located outside of Brevard County, for the said evidence herein described, and for the seizure, safekeeping, and examination thereof, subject to the order of this Honorable Court by duly constituted officers of the law.

Det. J Graves 125

Detective Jennifer Graves #125
Palm Bay Police Department
Affiant

SWORN TO AND SUBSCRIBED BEFORE ME THIS 10 DAY OF Sept, A.D. 20 19 BY Detective Jennifer Graves #125 (Affiant) WHO IS PERSONALLY KNOWN TO ME OR WHO PRODUCED _____ AS IDENTIFICATION.

SGT M Heatherly #763/2019

SWORN LAW ENFORCEMENT OFFICER
BREVARD COUNTY, FLORIDA